Continuous variable quantum cryptography using coherent states

Frédéric Grosshans and Philippe Grangier
Laboratoire Charles Fabry de l'Institut d'Optique (CNRS UMR 8501) F-91403 Orsay, France

We propose several methods for quantum key distribution (QKD), based upon the generation and transmission of random distributions of coherent or squeezed states. We show that these protocols are secure against individual eavesdropping attacks, provided that the transmission of the optical line between Alice and Bob is larger than 50 %. The security of the protocol is related to the no-cloning theorem, that limits the signal to noise ratio of possible quantum measurements on the transmission line, even though the transmitted light has no "non-classical" feature such as squeezing. We show also that our approach can be used for evaluating any QKD protocol using light with gaussian statistics.

PACS numbers: 03.65.bz,42.50 Dv,89.70.+c

Since the experimental demonstration of quantum teleportation of coherent states [1], a lot of interest has arisen in continuous variable quantum information processing. In particular, a stimulating question is whether quantum continuous variables (QCV) may provide a valid alternative to the usual "single photon" quantum key distribution schemes [2]. Most present proposals to use QCV for QKD [3–15]. are based upon the use of "non-classical" light beams, such as squeezed light, or pairs of light beams that are correlated for two different quadratures components (the so-called "EPR" beams, by analogy with the historical paper by Einstein, Podolski and Rosen [16]). But recent work on this subject [17] underlined the crucial importance of the continuous variable version of the no-cloning theorem [18], as soon as security is concerned in any exchange using QCV.

In this letter, we show that there is actually no need for squeezed light : an equivalent level of security may be obtained by simply generating and transmitting random distributions of coherent states. The security of this novel protocols is related to the no-cloning theorem, that limits possible eavesdropping even though the transmitted light has no "non-classical" feature such as squeezing. We show that our analysis can be also applied to other protocols using light with gaussian statistics, *i.e.* squeezed or EPR beams, making thus the comparison easier. The basic tools for this analysis are the ones that have been extensively used for linearized quantum optics, including in particular optical quantum non-demolition (QND) measurements [19]. Before presenting our protocol, we will briefly review the current literature on continuous variables QKD.

Gottesmann and Preskill [3] recently proposed an unconditionnally secure continuous variable QKD. This scheme is based on error correcting codes, but its experimental implementation is not straightforward. Our approach is much simpler, but we will prove security against individual attacks only. Among these simpler approaches, Hillery proposed a QKD scheme based on binary modulated squeezed light [4]. Cerf *et al* showed it could be improved considering gaussian modulation [5,6] and described a reconciliation protocol [6,7] to implement this improved protocol. In the present work we will generalize this approach to the various single beam protocols of the litterature [4,8–14]. The protocol described in [5,6] is then a particular member of the family of protocols described here. EPR beam were also considered for QKD schemes. Some schemes need the propagation of one beam only from Alice to Bob [9–14], the other half of the EPR pair being measured by Alice, wheras others need the propagation of two modes (or more) of the electromagnetical field [8,12,13,15]. In the first family, Reid [10] and Ralph [9] consider "binary" modulated EPR beams, created by a parametric amplifier with a modulated seed [10] or interfering modulated squeezed beams [9], whereas Silberhorn *et al* [11,12] and Navez *et al* [14] extract their key from correlated measurement sequences. As we will show below, these schemes can be viewed as the transmission of a modulated sub-shotnoise beam. Bencheikh *et al* [13] extract the binary key directly from the gaussian correlations. This extraction can be optimized using the reconciliation protocol described in [6,7]. The protocols transmitting several quantum-correlated modes of the electromagnetic field, using two beams [8,12,13,15] are beyond the scope of this letter, because their security analysis should take into account simultaneous attack on both modes. However, similar gaussian extension of these protocols seem possible. Finally, Ralph examined a binary modulated coherent beam protocol [8,9] and showed its limited security. But we will show now that its gaussian extension is as secure and as efficient as other one-beam squeezed light or EPR protocols.

General principle of the protocols. The QKD protocols we study here are single gaussian beam protocols. Alice modulate randomly a gaussian beam and send it to Bob through a gaussian noisy channel. Both phase and amplitude are modulated with gaussian random numbers, since it allows an optimal information rate [20]. Bob then measures either the phase or the amplitude of this beam and informs Alice which measurement he made. Bob and Alice have then two correlated sets of gaussian variables, from which they can extract a common secret string of bits as explained below.

The basic tool that we will use is the Shannon formula giving the optimum information rate I of a noisy transmission channel, in units of bits/symbol [20]. If the noise is white and gaussian and the signal to noise ratio (SNR) is Σ, this optimum information rate is

$$I_{AB} = 1/2 \log_2(1+\Sigma). \quad (1)$$

Since this optimum can be closely approached only if the signal has a gaussian statistics [20], we will consider only gaussian modulation protocols, and use (1) to calculate the amount of private information that Alice and Bob may exchange in presence of the eavesdropper Eve.

The sliced reconciliation protocol described in detail in [6,7] and briefly sketched in the Appendix allows us to get arbitrarly close to the value given by (1). For security purposes, one must assume that Eve has an arbitrary powerful computer, and thus she is able to reach this limit. In case Alice and Bob are not, they will have to allow for an extra security margin (see *Discussion* below). We note that it is not required to specify a "digitizing step" to connect the continuous variable and a bit value: it is simply assumed that this digitizing step is smaller than the channel noise, so that the information rate is indeed determined by the channel signal to noise ratio. The bits will appear at the end of the reconciliation protocol [6,7]. At this stage, Alice and Bob share a string of bits which is partly known by Eve. They can then use standard privacy amplification protocol [22] to agree on a secret key. The rate at which this secret key can be constructed is

$$\Delta I = I_{AB} - I_{AE}, \quad (2)$$

where I_{AB} (I_{AE}) is the information rate between Alice and Bob (Eve).

Eavesdropping. The I_{AB} term of (2) is easy to compute for a given scheme, the signal to noise ratio Σ_B being known. We have to assume I_{AE} being the maximum possible given the laws of physics (considering only individual attacks, coherent attacks are beyond the scope of this letter). If the protocols are symetric in X and P, the best tactic for Eve is to keep this symmetry in her attacks. Therefore, we can restrict us to attacks symmetric in quadrature without loss of generality.

Given these hypothesis, we will use a general result, that is demonstrated in [17] : if the added noise on Bob's side is χN_0, where N_0 is the vacuum noise variance, then the minimum added noise on Eve's side is $\chi^{-1} N_0$. This applies to both quadratures, and the added noise may be due to line losses, eavesdropping, or any other reason [17]. Since the demonstration of ref. [17] is just another form of the no-cloning theorem, it also adresses any individual attack by Eve using a cloning machine [18]. Since the best Eve can do is to use a symmetric cloning machine, the same noise is added to both quadratures of the light beam, both for Eve's eavesdropped data and for the remaining data sent out to Bob. In the simplest case of a beam-splitting attack, where Eve takes a fraction $1-\eta$ of the beam and sends η to Bob, one has $\chi = (1-\eta)/\eta$.

Equation (2) shows that these protocols are secure as long as Bob has a more in formation on Alice's key element than Eve, *i.e.* as long as $I_{AB} > I_{AE}$. Since the Shannon formula (1) is valid for both Bob and Eve, the security condition is just a condition on the signal to noise ratios, which turns to be a condition on the added noises, since the signal and the noise added at Alices side (quantum noise, Alice's technical noises) are the same. If the noise added by Bob's measurement is considered as a transmission noise (which is pessimistic), we have

$$\Delta I > 0 \Leftrightarrow \Sigma_B > \Sigma_E \Leftrightarrow \chi < 1 \Leftrightarrow \eta > 1/2 \quad (3)$$

Therefore, a usable key can be obtained in principle as soon as the transmission losses are less 3dB. Taking into account the standard loss of 0.2dB/km in optical fibers at 1550 nm, the typical range would be around 10 km.

In this security evaluation, the noise added in Alice's side cancels out because it disturbs equally Eve and Bob. This 'cancelled' noise includes the quantum noise of the beam. *The security of these protocols relies of the quantum aspects of measuring or copying, but not on any quantum feature of the beam, like squeezing or entanglement.* We can do quantum cryptography with coherent beams, as mentionned by Ralph [8,9] or even with highly noisy beams. Quantum features of the beams might influence some characteristics of the protocol like the secret key rate or the amount of classical communication needed to agree on the secret key, but not its security.

Coherent Beam protocol. Let us now explicitly describe the coherent beam protocols of this family:

1. Alice draws two random numbers x_A and p_A from a gaussian law with variance $V_A N_0$
2. She sends to Bob the coherent state $|x_A + i p_A\rangle$
3. Bob randomly chooses to measure either X or P. This measurement can be done perfectly.
4. Using a classical public channel he informs Alice about the observable that he measured (like in the BB84 protocol, half of the key generated by Alice is unused)
5. Alice and Bob share two correlated gaussian variables. Then they may use the "sliced reconciliation" protocol [7,6] to transform it into errorless bit strings. Finally, they have to use a standard protocol for privacy amplification [22] in order to distill the private key.

According to eq. (1), the channel rate ΔI for the private key will be:

$$\Delta I = \tfrac{1}{2}\log_2(1+\Sigma_B) - \tfrac{1}{2}\log_2(1+\Sigma_E) \quad (4)$$

The total variance of any quadrature of the beam when it leaves Alice's realm is $V N_0 = V_A N_0 + N_0$. Using the expressions $1+\Sigma_B = \frac{V+\chi}{1+\chi}$, and $1+\Sigma_E = \frac{V+1/\chi}{1+1/\chi}$, the useful secret information rate is :

$$\Delta I = \tfrac{1}{2}\log_2 \tfrac{V+\chi}{1+V\chi} \quad (5)$$

If $\chi < 1$, ΔI will increase as a function of the signal modulation V_A. For large modulation ($\chi V_A \gg 1$), the asymptotic value of ΔI is :

$$\Delta I_{asymp} = -\tfrac{1}{2}\log_2 \chi = \tfrac{1}{2}\log_2 \tfrac{\eta}{1-\eta} \quad (6)$$

while the raw channel rate between Alice and Bob is $I_{AB} = \frac{1}{2}\log_2(V/(1+\chi))$.

Squeezed state protocol. This protocol can straightforwardly be generalized to modulated squeezed beam, with a squeezing factor $s < 1$. The protocol becomes :

1. Alice chooses randomly if the beam is squeezed in X or P (for instance we will later assume the beam being X-squeezed). Let denote $|\psi\rangle$ this squeezed state.

2. Alice draws two random numbers x_A and p_A from two gaussian laws with variances $V_{x_A}N_0$ and $V_{p_A}N_0$. The two squeezed direction are indistinguishable for Eve iff

$$V_{x_A}N_0 + sN_0 = V_{p_A}N_0 + \frac{1}{s}N_0 \equiv VN_0 \tag{7}$$

3. Alice sends to Bob the displaced squeezed state $D(x_A + ip_a)|\psi\rangle$

4. Bob randomly chooses to measure either X or P.

5. Using a public channel, Alice and Bob inform each other about the squeezing direction and the measured observable.

6. Like with coherent states Alice and Bob share correlated gaussian variables, from which they can extract a private binary key.

This protocol obviously reduces to the protocol described above if $s = 1$. Another limit, where $V_{p_A} = 0$ or $V = 1/s$, is the protocol described by Cerf *et al* in [5,6]. In this case, information is gathered for the key only when Bob makes the right guess.

To compute the private rate ΔI, we will average between the right guesses and the wrong guesses :

$$\Delta I = \tfrac{1}{2}[(I_{ABX} - I_{AEX}) + (I_{ABP} - I_{AEP})] \tag{8}$$

$$= \tfrac{1}{4}\log_2 \tfrac{(1+\Sigma_{BX})(1+\Sigma_{BP})}{(1+\Sigma_{EX})(1+\Sigma_{EP})} \tag{9}$$

We have $\Sigma_{BX} = \frac{V_{x_A}}{s+\chi} = \frac{V-s}{s+\chi}$ and $1 + \Sigma_{BX} = \frac{V+\chi}{s+\chi}$. The three other signal to noise ratios are obtained by replacing χ or/and s by χ^{-1} or s^{-1}. Therefore,

$$I_{AB} = \tfrac{1}{4}\log_2 \tfrac{(V+\chi)^2}{\chi} - \tfrac{1}{4}\log_2(\chi + \tfrac{1}{\chi} + s + \tfrac{1}{s}) \tag{10}$$

$$I_{AE} = \tfrac{1}{4}\log_2 \tfrac{(V+1/\chi)^2}{1/\chi} - \tfrac{1}{4}\log_2(\chi + \tfrac{1}{\chi} + s + \tfrac{1}{s}) \tag{11}$$

Since the s-dependent term of these information rates are the same, they cancel each other in ΔI. The secret information rate is thus again given by eq. (5), and does not depend on the degree of squeezing.

Extension to EPR case. The previous description does not apply directly on EPR protocols. However, an EPR QKD protocol where Alice keeps one of the beams and sends the other to Bob is logically equivalent to a randomly modulated beam with a sub-shot noise quantum variance. Let note X_A the quadrature Alice measures and X_{out} the same quadrature of the beam sent to Bob when it leaves Alice's lab. For a standard non-modulated EPR scheme [11] we have the following relations :

$$\langle X_A^2 \rangle = \langle X_{out}^2 \rangle \equiv V = (s + 1/s)/2 \tag{12}$$

$$\langle (X_A - X_{out})^2 \rangle = 2s \tag{13}$$

$$\langle X_A X_{out} \rangle = V - s \tag{14}$$

We can separate Bob's beams in two parts, that are respectively correlated and uncorrelated with Alice's measurement, by writing $X_{out} = gX_A + N$ where $\langle X_A N \rangle = 0$. Bob's beam is then equivalent to a beam with quantum noise $\langle N^2 \rangle$ on quadrature X, which is randomly modulated with the variable gX_A. Using eqs (12,14) one gets:

$$g = 1 - s/V = (1 - s^2)/(1 + s^2) \tag{15}$$

$$\langle N^2 \rangle = s(2 - s/V) = 2s/(1 + s^2). \tag{16}$$

These equations describe the case where Alice and Bob measure the same quadrature. When Alice changes her quadrature, while Bob keeps the same measurement, the initial wave packet is reduced onto a noisy quadrature, and no useful correlation is generated. On the average, the information rate is therefore half of the "equivalent" modulation scheme. Using (12), we have then:

$$1 + \Sigma_B = 1 + \frac{g^2 V}{\langle N^2 \rangle + \chi} = \frac{V(V+\chi)}{1+\chi V} \tag{17}$$

$$\Delta I = \tfrac{1}{4}\log_2(\tfrac{V+\chi}{1+\chi V}\tfrac{1+V/\chi}{V+1/\chi}) = \tfrac{1}{2}\log_2(\tfrac{V+\chi}{1+\chi V}) \tag{18}$$

This value of ΔI is again just the same as the coherent state result (5) for given χ and V, so that s is defined by (12). Adding excess noise or a modulation on the outgoing beam brings no further improvement.

Discussion. Various comments are in order. First, it appears that non classical features like squeezing or EPR correlations have no influence on the achievable secret key rate for the family of protocols that were described here. This result may not apply to all possible protocols, *e.g.* , we did not consider using a continuous quantum memory. On the other hand, since the raw information rate are different for the same secret key rate, squeezed beams can be used to save classical communications during the privacy amplification procedure. The EPR beams have also the advantage of directly providing quantum-generated gaussian noise, rather than having it externally generated by Alice. More importantly, entanglement, that is not directly used in the present protocols, can be useful to beat the 3 dB limit by using more than one beam. Though the 3 dB loss limit of our cryptography protocols makes their security demonstration quite intuitive, there exist multiples ways for Alice and Bob to go beyond this limit. The most radical way is to send many EPR beams through the noisy channel, then to use entanglement purification [21] to build stored entanglement between Alice and Bob, and finally to implement a high fidelity teleporter. For any finite value of the losses and EPR entanglement, an arbitrarily high fidelity can be achieved [21]. The no-cloning theorem ensures the security of these schemes as soon as the fidelity of the teleporter is above 2/3 [17], which is equivalent to the 3 dB loss limit discussed above. In some sense, a "lossless" line is re-created by using entanglement purification. There may exist more realistic ways to cross the 3 dB barrier. For instance, Alice and Bob may "invert" the reconciliation procedure, with Alice guessing Bob's measurement instead of Bob guessing

Alice's value [22]. This inverted procedure may be more efficient, but its complete security analysis is beyond the scope of this letter.

On the practical side, one should note that Bob's detectors are not ideal, but have a non-zero electronic noise B_0, that should be much smaller than N_0, and a maximum (saturation) input power $\sigma B_0 \gg N_0$, where $\sigma \gg 1$ is the detector's dynamics. Taking into account these characteristics in the simplest coherent state protocol gives an optimum value of the signal variance, $V_A \sim \sqrt{\sigma}$. Another point is that Alice and Bob may not be able to achieve the Shannon limit (1), due to limited computing power (so such limitation is relevant for Eve). Assuming that the effective information rate between Alice and Bob is reduced by a factor $\alpha < 1$, the net secret rate becomes $\Delta I_{eff} = \alpha I_{AB} - I_{AE}$, and remains positive if $\alpha > I_{AE}/I_{AB}$. The quantity ΔI_{eff} is plotted on Fig.1 for $\alpha = 1$ (full lines), and for various values of α that are arbitrarily associated with various values of the SNR (dashed lines). It is clear from that figure that low values of α reduce the transmission range in which the protocol is secure. We note that according to [6,7], the sliced reconciliation protocol should yield $\alpha \sim 1$ (see also Appendix), but this may be costly in terms of calculation time and public channel transmissions. All these constraints should eventually be taken into account to choose the most appropriate value of V_A.

As a conclusion, it is possible to design a QKD scheme with coherent states, secure against any individual attack, by using optimized reconciliation protocols and privacy amplification. Our protocol, where Bob makes a random choice of the measured observable and sends later his choice to Alice, has many analogies with BB84. If the protocol is implemented by sending light pulses like in a coherent telecommunication scheme, all pulses will be useful, but half of information sent by Alice will be lost. We demonstrated that the protocol is secure for losses smaller than 3dB (or a teleportation fidelity larger than 2/3 [17]), and the net information rate for the private key with a large signal modulation is $1/2 \log_2(1/\chi) = 1/2 \log_2(\eta/(1-\eta))$.

Appendix : Sliced reconciliation protocol

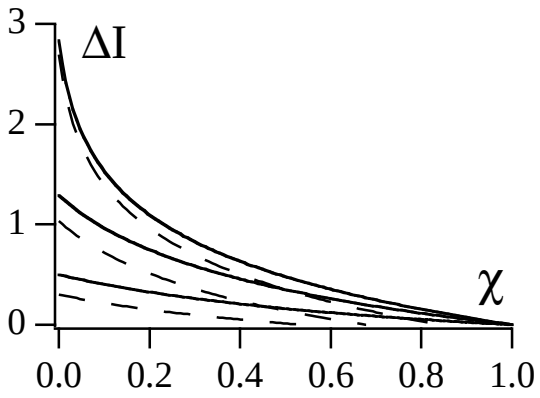
In the n-slice version of the reconciliation protocol proposed in ref. [7], the real axis representing the amplitude of the signal is split in 2^n intervals $s_1 =]-\infty,\ -t_1]$, $s_2 =]-t_1,\ -t_2]$, ... $s_{2^n} =]t_{2^n-1},\ +\infty[$, where $t_p = -t_{2^n-p}$, and $t_{2^{n-1}} = 0$. Alice assigns an amount of n bits to an amplitude that lies in the interval s_p, by using the parity of p for bit 1, of $Floor(p/2)$ for bit 2, ... , and of $Floor(p/2^{n-1})$ for bit n. After receiving the data, Bob makes an optimized guess of the first bit value using appropriate weighting functions, that are computed by optimizing the choice of the $\{t_p\}$ (this optimization is made only once, before exchanging the data). After a first correction round by exchanging public data between Alice and Bob, Bob knows the correct value of the first bit. Then he tries to guess the second bit, with a much higher probability of success, because he already knows the first one. By increasing both the SNR Σ and the number of slices, the process gets more and more efficient, keeping the same main idea : after each correction round, Bob can guess the next bit with a higher probability. For the 5-slice protocol with $\Sigma = 15$ presented in [7], the probabilities of guessing right for slices 4 and 5 are respectively 0.976 and 0.999994, and the efficiency is more than 90% of the Shannon limit $\frac{1}{2}\log_2(16) = 2$.

Acknowledgments. This work was carried out in the framework of the European IST/FET/QIPC project "QuICoV". We are grateful to N.J. Cerf and G. van Assche for helpful discussions.

[1] A. Furusawa *et al* , Science **282**, 706 (1998).
[2] For a review see *e.g.* W. Tittel, G. Ribordy, and N. Gisin, Physics World, p. 41 (march 1998)
[3] D. Gottesmann and J. Preskill, Phys. Rev. A **63**, 022309 (2001)
[4] M. Hillery, Phys. Rev. A **61**, 022309 (2000)
[5] N.J. Cerf, M. Lévy and G. van Assche, Phys. Rev. A **63**, 052311 (2000)
[6] N.J. Cerf, S. Iblisdir and G. van Assche, e-print quant-ph/0107077, submitted to Eur. Phys. J. D (2001)
[7] G. van Assche, J. Cardinal and N.J. Cerf, e-print cs.CR/0107030, submitted to IEEE (2001)
[8] T.C. Ralph, Phys. Rev. A **61**, 010303(R) (2000)
[9] T.C. Ralph, Phys. Rev. A **62**, 062306 (2000)
[10] M.D. Reid, Phys. Rev. A **62**, 062308 (2000)
[11] Ch. Silberhorn, N. Korolkova and G. Leuchs, e-print quant-ph/0109009 (2001)
[12] S. Lorenz *et al* , e-print quant-ph/0109018 (2001)
[13] K.Bencheikh, Th.Symul, A.Jankovic and J.A.Levenson, to appear in J. Mod. Optics (2001)
[14] P. Navez, A. Gatti and L.A. Lugiato, e-print quant-ph/010113 (2001)
[15] S.F. Pereira, Z.Y. Ou and H.J. Kimble, Phys. Rev. A **62**, 042311 (2000)
[16] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935)
[17] F. Grosshans and Ph. Grangier, Phys. Rev. A **64** 010301(R) (2001)
[18] N.J. Cerf and S. Iblisdir, Phys. Rev. A **62**, 040301(R) (2000)
[19] Ph. Grangier, J.-A. Levenson and J.-Ph. Poizat, Nature **396**, 537 (1998).
[20] C.E. Shannon, Bell Syst. Tech. J. **27** 623-656(1948)
[21] L.-M. Duan *et al* , Phys. Rev. Lett. **84**, 4002 (2000).
[22] U. Maurer and S. Wolf, *Advances in Cryptology-EUROCRYPT'00*, Lecture Notes in Computer Science **1807**, 351-368, Springer Verlag (2000)

Figure

FIG. 1. Private channel information rate ΔI as a function of the channel noise χ. The three curves in full lines correspond to $V_A = 1, 5, 50$ from the bottom to the top, assuming that the reconciliation protocol between Alice and Bob reaches the Shannon limit. The three curves in dashed lines correspond to the effective ΔI with the sames values of V_A, with (arbitrarily chosen) reconciliation efficiencies α that are respectively 0.6, 0.8 and 0.95 of the Shannon limit.


3
ΔI
2
1
0
χ
0.0
0.2
0.4
0.6
0.8
1.0